Security Challenges in Manycore Embedded Systems based on Networks-on-Chip (NoCs)

Ermis PAPASTEFANAKIS
Bruno MAITRE
Dominique RAGOT

firstname.lastname@thalesgroup.com

www.thalesgroup.com
Outline

- Thales at a glance
- Security context (evaluation of products)
  - A view on security
  - Evaluation
- Internal projects
  - Problems definition
- R&D (collaborative projects)
  - Projects, objectives and challenges
  - Future directions
- Conclusions
Markets we serve

DUAL MARKETS
Military & Civil

TRUSTED PARTNER FOR A SAFER WORLD
Product lines

- Radio Communications
- Networks & IT Infrastructures
- Critical Information Systems and Cybersecurity

Applications:

- Resilient networks
- Real-time image processing (airports, critical infrastructure protection, events)
- Global & local situation awareness (smart cities)
- Cryptography
Products evolution

Legacy systems

- Single processor architectures
- One OS per processor
- Redundant networks for different criticality flows

Future systems requirements

- Integration on a Multi-Processor SoC
  - Resource sharing
  - Size provisioning
- Co-existence of secure and non-secure tasks or OSs
  - Isolation between the two worlds
  - Hypervisor manages accesses
  - Optimal task scheduling and placement
- Different criticality flows on the same network
Current embedded platforms

### Multicore

- **ARM-based**
  - Freescale iMX6 (Up to 4 cores)
  - Cavium ThunderX
- **PowerPC-based**
  - Freescale P4080 (Up to 8 cores)
- **DSP platforms**
  - Media encoding/decoding platforms (Up to 24 cores)

### Manycore

- Adapteva: Parallela (64 cores)
- EZChip (Ex.Tilera) TILE-Gx8072 (72 cores)
- Kalray: MPPA256 (256 VLIW cores)
Security

IP elements
- Random Number Generators (RGNs)
- Hardware Security Modules (HSMs)
- Trusted Execution Environment (TEE)

Assets to protect
- Hypervisor
- OS
- User data
- Monitoring data

Architectural elements
- Memory Management Unit (MMU)
- Input/Output MMU
- Cache hierarchy
- Interconnect
- Power management
Security test and protection

<table>
<thead>
<tr>
<th>Physical</th>
</tr>
</thead>
<tbody>
<tr>
<td>➢ Electromagnetic emissions</td>
</tr>
<tr>
<td>➢ Thermal scanning</td>
</tr>
<tr>
<td>➢ Power analysis (SPA, DPA)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Architectural</th>
</tr>
</thead>
<tbody>
<tr>
<td>➢ Timing analysis (Side channel attack)</td>
</tr>
<tr>
<td>➢ Cache trashing (DoS)</td>
</tr>
<tr>
<td>➢ Illegal accesses (DoS)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>➢ Inherent design vulnerabilities</td>
</tr>
<tr>
<td>➢ 3rd party, untrusted</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hardware protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>➢ Flow randomization</td>
</tr>
<tr>
<td>➢ Isolation/Partitioning</td>
</tr>
<tr>
<td>➢ Quality of Service</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Software protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>➢ Manage access requests</td>
</tr>
<tr>
<td>➢ Detect abnormal behavior</td>
</tr>
<tr>
<td>➢ Reinitialize / Disable faulty IPs</td>
</tr>
</tbody>
</table>
Security evaluation

- **Common Criteria**
  - Recognized internationally (25 countries)
  - 7 Evaluation Assurance Levels (EAL1-7 higher is better)

- **Evaluated products**
  - Smartcards (EAL4-EAL7)
  - IP elements (EAL7 ex. Memory Management Unit SAMSUNG S3FT9KF)
  - Trusted platform modules (EAL4)

- **Alternatives**
  - FIPS-140-2 (USA & Canada)
    - 4 levels
  - Certificat de Securité de Premier Niveau (CSPN) (France)

Small systems with low complexity
Need to evaluate bigger systems
Current work

- **Real-time audio/video**
  - Communication terminals
  - Control terminals

- **Mixed criticality flows**
  - Embedded router

- **Secure content**
  - In-Flight Entertainment systems
  - Set top boxes
Future work

- Adapt production tools
  - Applications parallelization
  - Compiler
  - Porting hypervisor/OS

- Mapping and migrating

- Communication impact

- Power management
Challenges

- **MPSoC scalability, HW accelerators**
  - Hypervisor overhead? Multiple hypervisors?
  - Maintain cache coherency? Hierarchy?

- **Sharing of peripheral controllers? (Network, Graphics)**
  - Multiple peripheral controllers?
  - Hardware Virtualization for Peripherals?

- **Isolation of different partitions**
  - Can Networks-on-Chip enhance isolation? (MLS)
  - Can partitions exchange information securely? (MILS)

- **How to evaluate?**
  - Avoid evaluating the whole system? Just the hypervisor and compiler?
  - Can isolation allow partial evaluation?
Collaborative projects

- **MPSoC scalability, HW accelerators**
  - Hypervisor overhead? Multiple hypervisors?
  - Maintain cache coherency? Hierarchy?

- **Sharing of peripheral controllers? (Network, Graphics)**
  - Multiple peripheral controllers?
  - Hardware Virtualization for Peripherals?

- **Isolation of different partitions**
  - Can Networks-on-Chip enhance isolation? (MLS)
  - Can partitions exchange information without leaks? (MILS)

- **How to evaluate?**
  - Avoid evaluating the whole system? Just the hypervisor and compiler?
  - Can isolation allow partial evaluation?
Current and future work

MPSoC scalability, HW accelerators
- GPPA offloading, code annotation, performance evaluation
- Security analysis on IOMMU evaluation potential with Common Criteria
- Network-on-Chip security evaluation, attack scenarios and counter measures proposals

Sharing of peripheral controllers? (Network, Graphics)
- Design and prototyping of a virtualizable secure network controller. Network traffic is isolated from one VM to another
- Design of a secure virtualizable DMA controller whose channels can be securely partitioned among VMs by the hypervisor.
- Secure and lightweight hypervision software for manycores.
Current and future work

**SAFURE** *(In progress 2015-2018) Safety and security*
- Achieve an integrated process to analyze, design, develop and validate security and safety constraints with applications in automotive and wireless/mobile communications.
- Achieve secure virtualization for GPUs

**MANGO** *(In progress 2015-2018) Isolation of different partitions (MILS, MLS)*
- Can Networks-on-Chip enhance isolation?
- Can partitions exchange information securely?
- Optimize task placement for security and timeliness?
Conclusions

- **Stronger security considerations in future Manycore research**
  - Architectural elements including security features

- **The aspect of evaluation can be useful in applied research**
  - Increase evaluation potential in models

- **Tighter connection between HW and SW**
  - Expose HW mechanisms at firmware/software level
  - Promote standards adoption in interfaces (ex. TPM)

- **Manycores as accelerators or as standalone systems?**
  - Enhance compilation and offloading to be “architecture-aware”
  - Allow multiple tasks or OSs to co-exist in isolation
Questions?